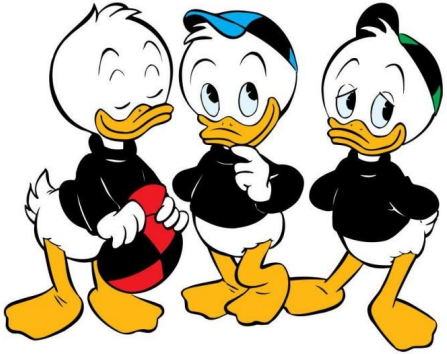
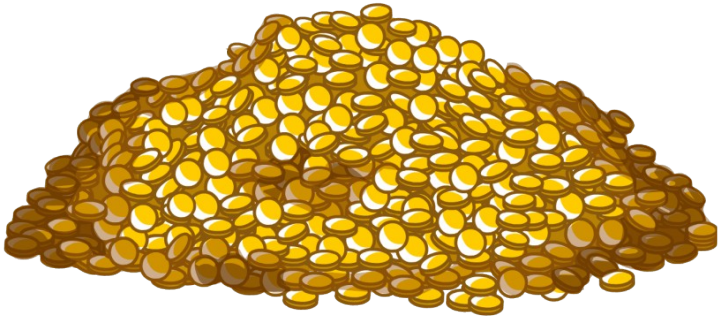
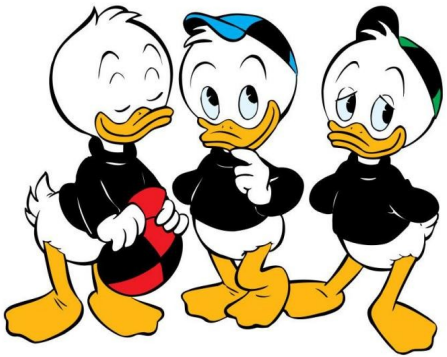
How To Share A Secret

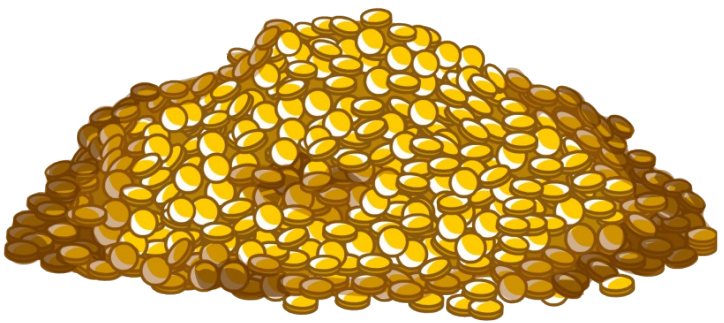
based on an equally named paper by Adi Shamir
(the S in RSA)


© Disney

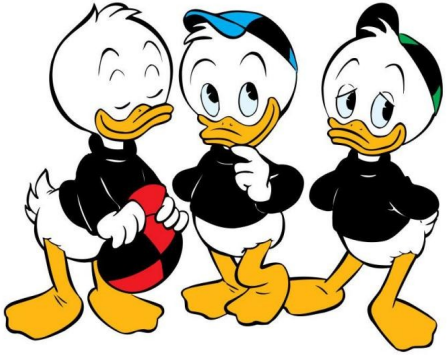


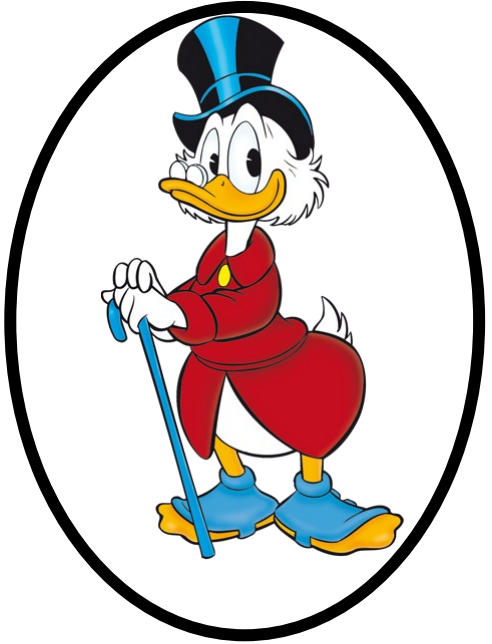


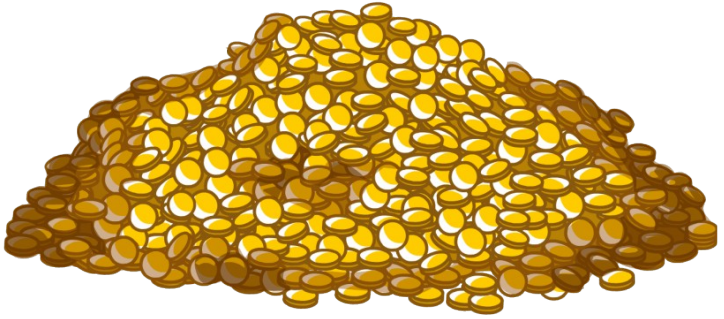


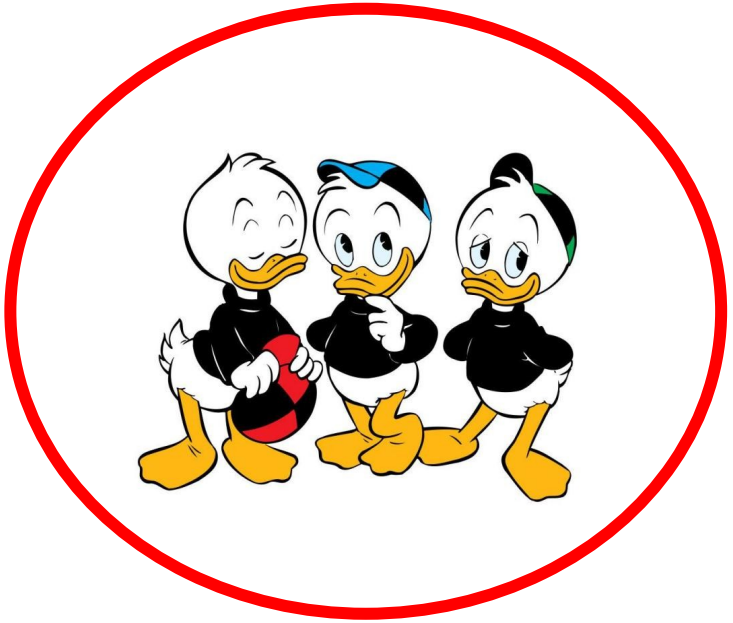


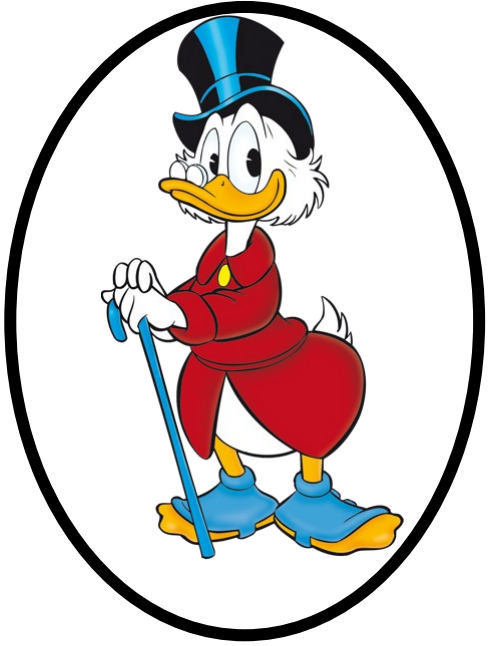
Everyone Gets Access Keys

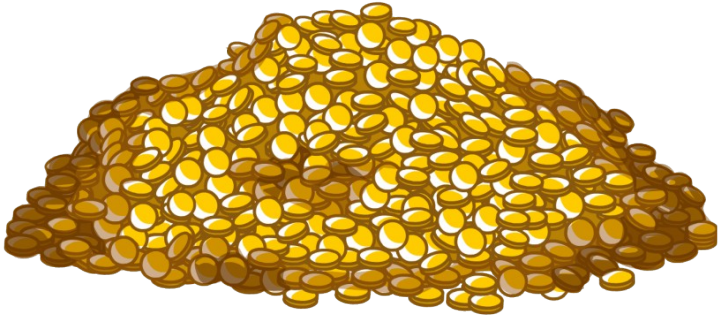


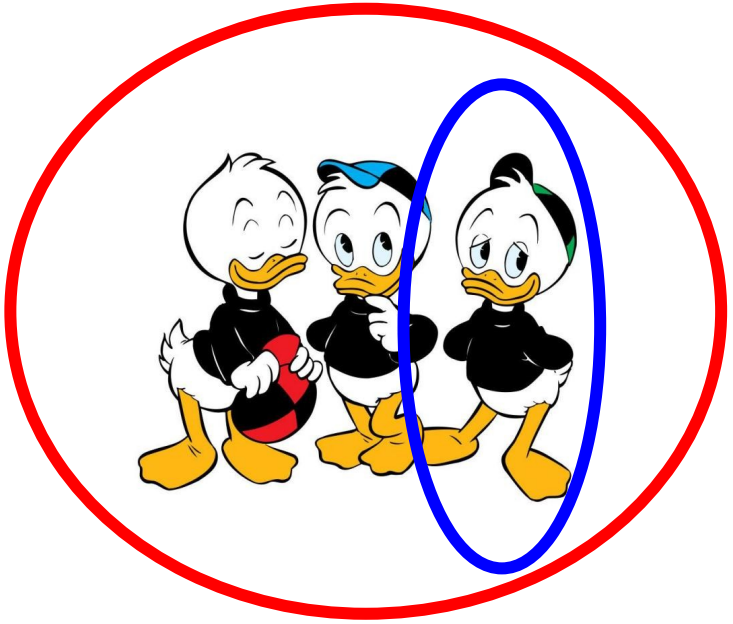


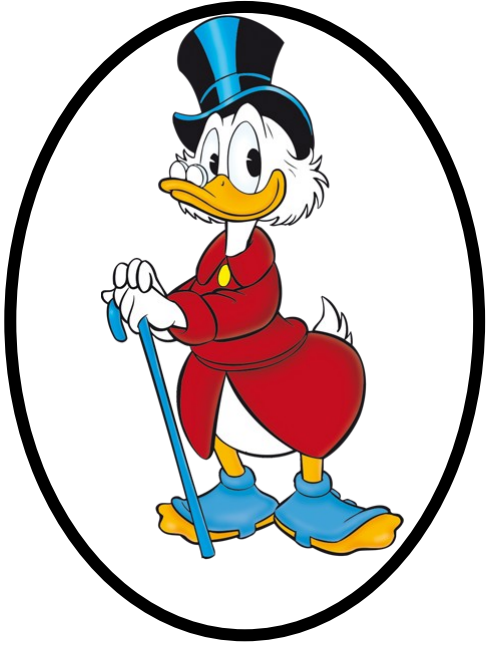


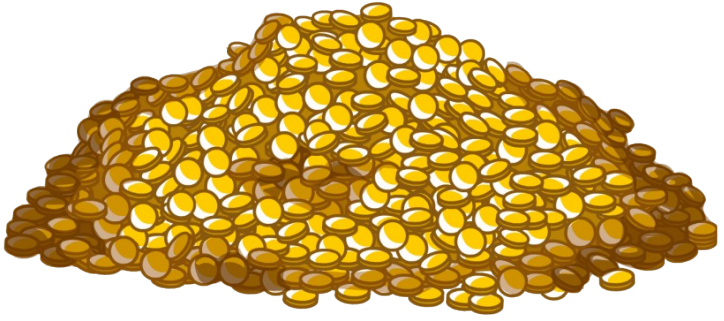


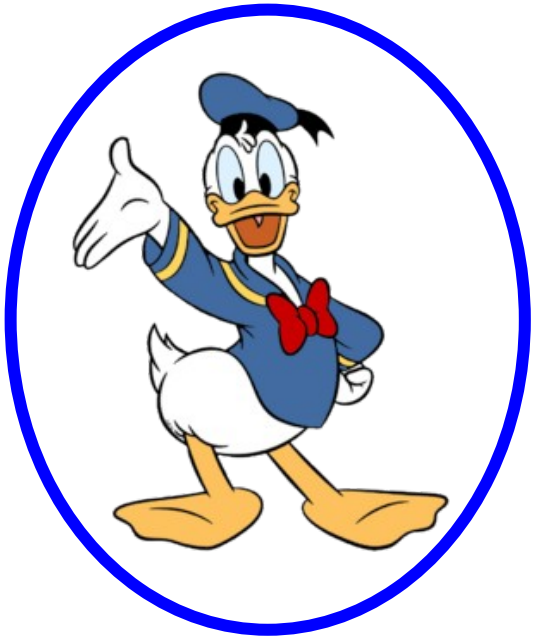


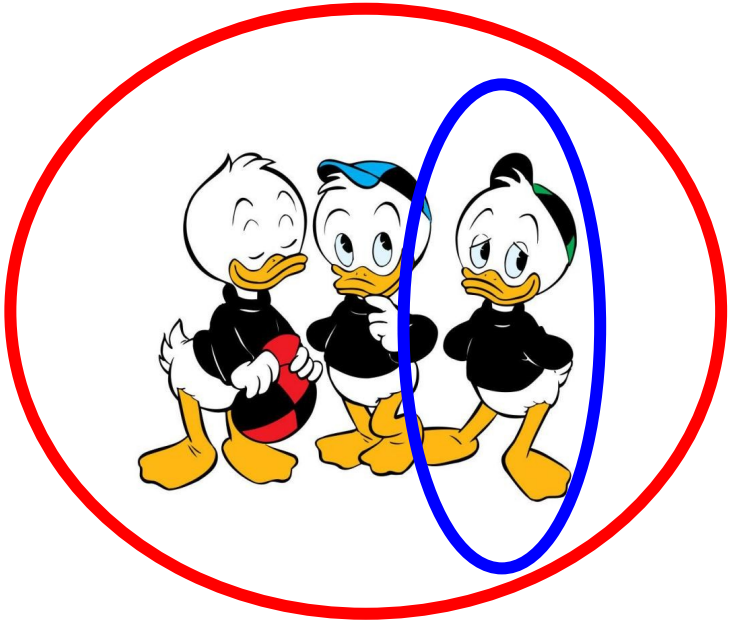


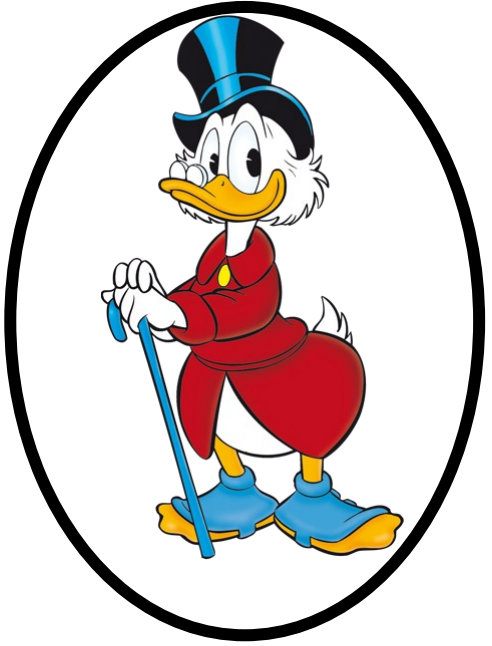


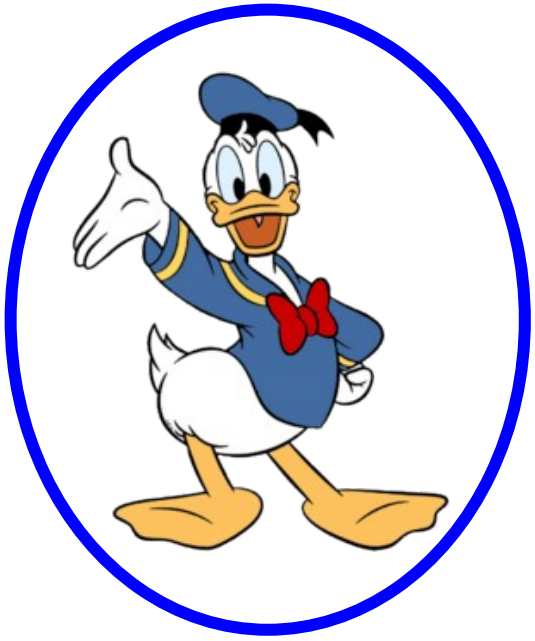


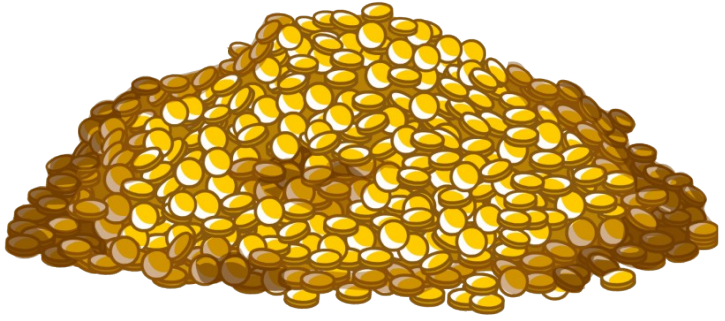




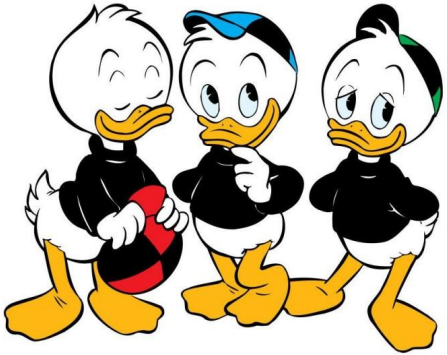




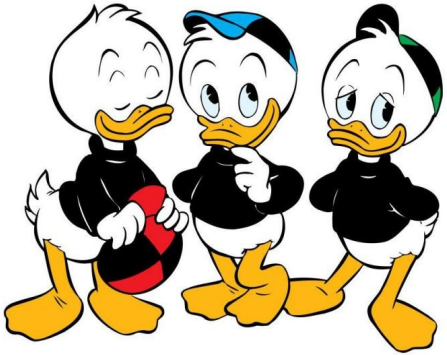




Hierarchical Access




76-167
76-671



Security Against Theft

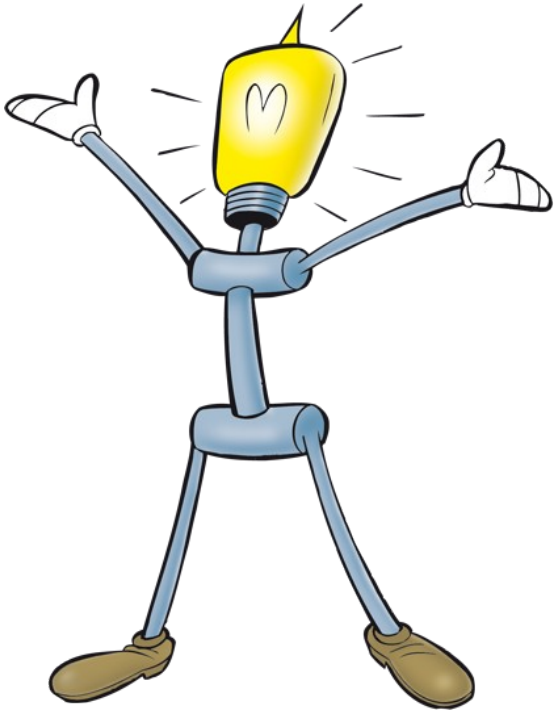
How?

One hidden master key for all?

How?

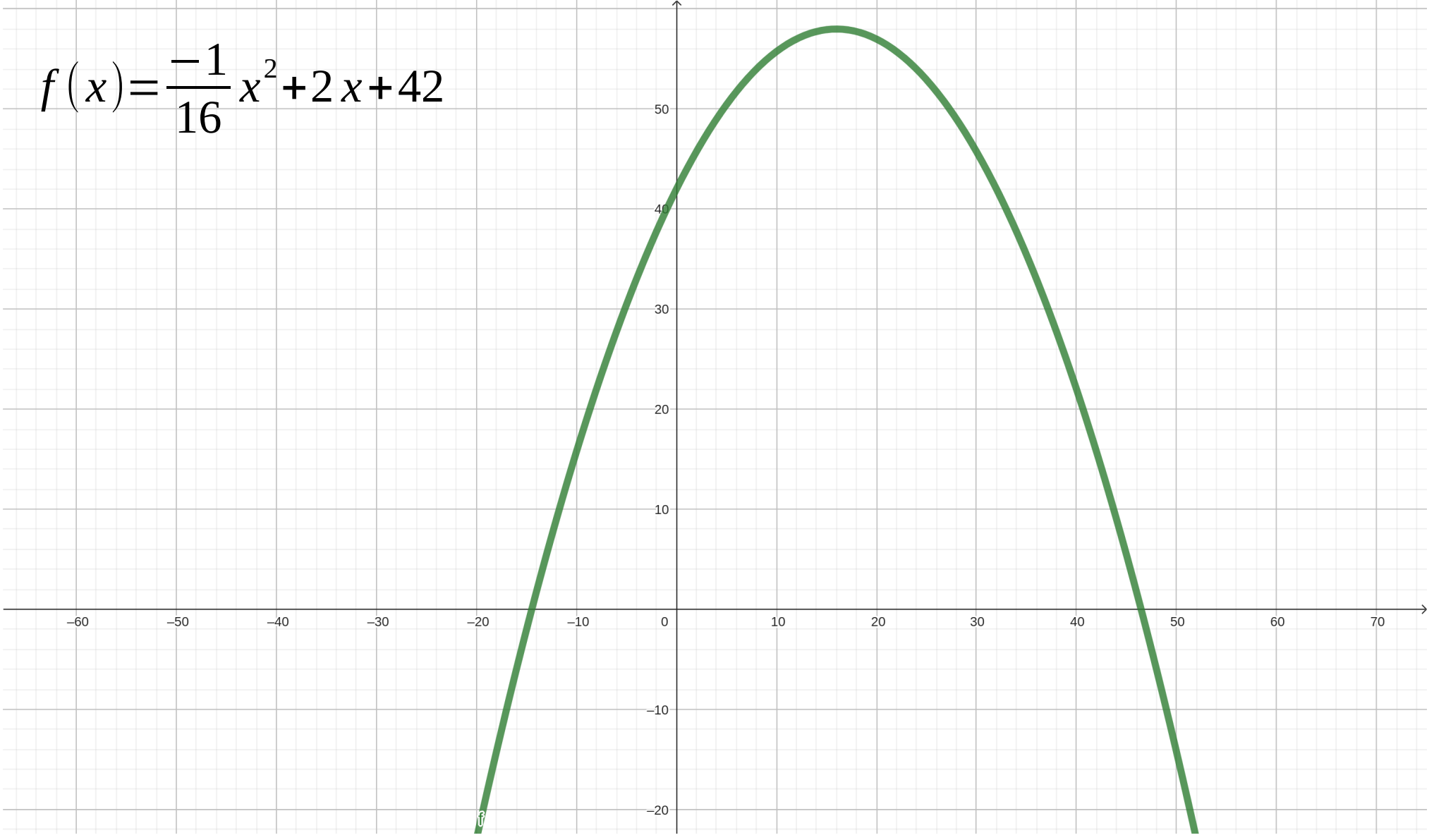
One hidden master key for all?
No hierarchy!
No security against theft or loss!

How?



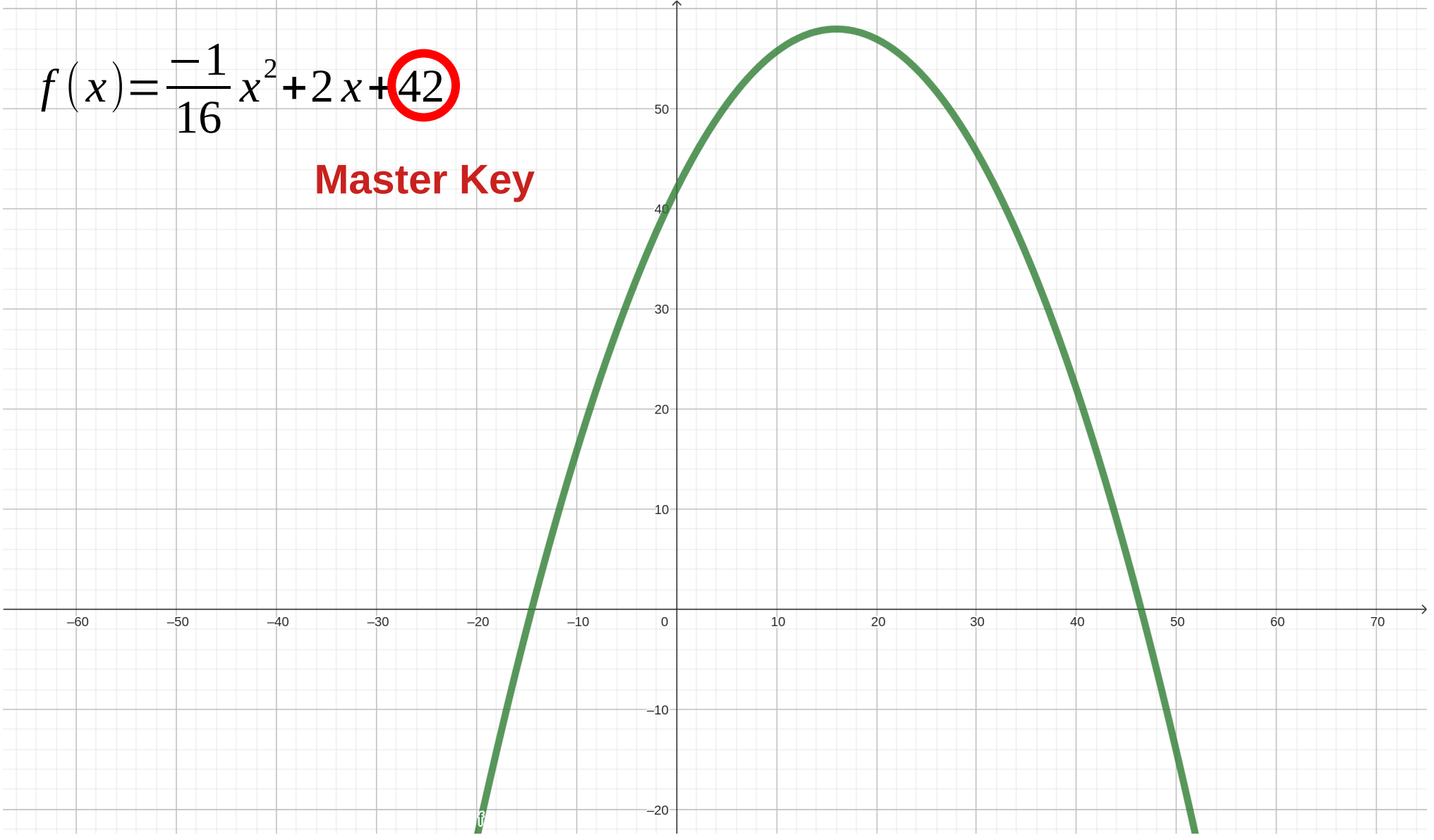
Use a **polynomial** (and a master key)**!**

$$f(x)=\frac{-1}{16}x^2+2x+42$$



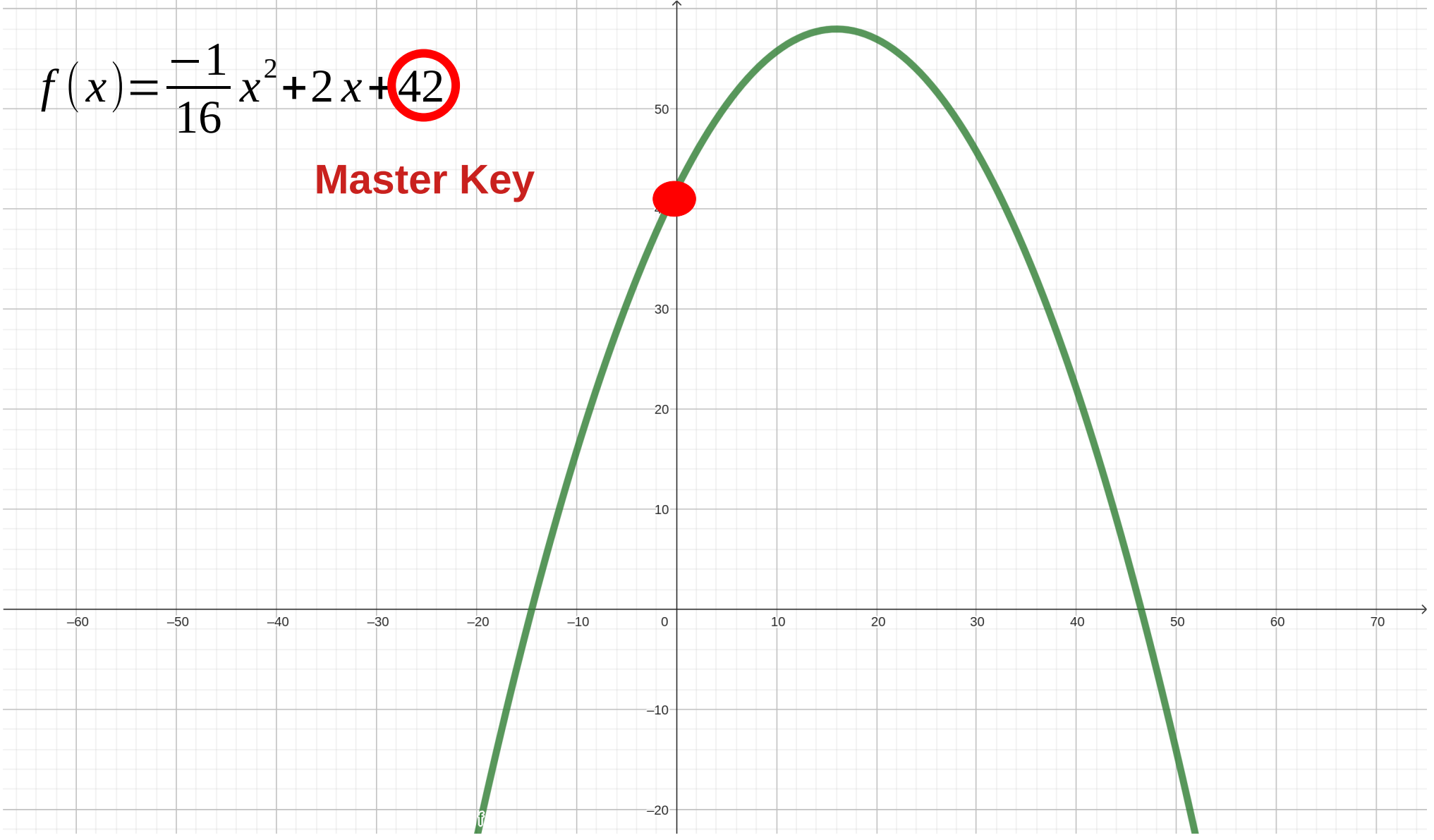
$$f(x)=\frac{-1}{16}x^2+2x+42$$

Master Key

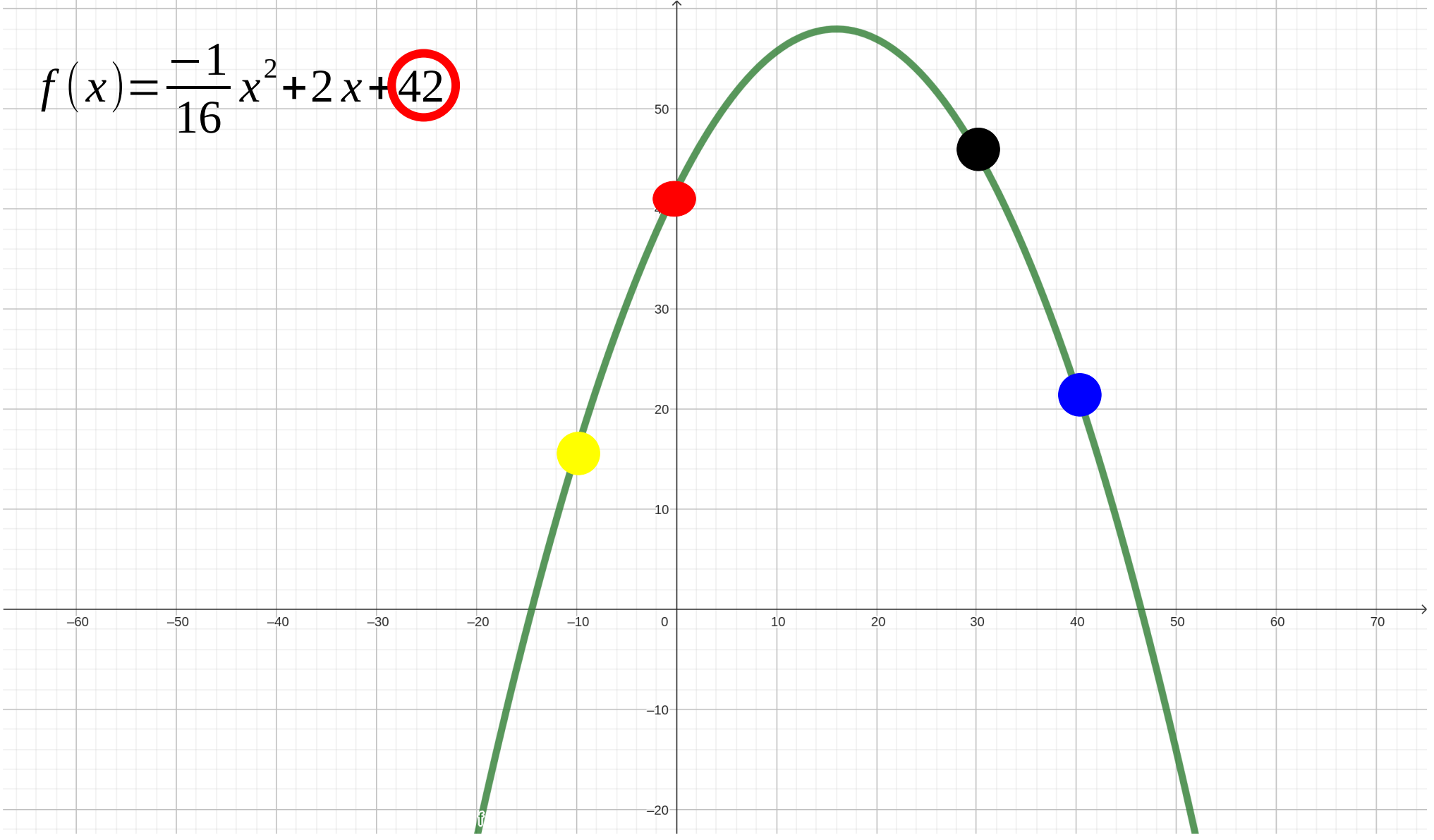


$$f(x)=\frac{-1}{16}x^2+2x+42$$

Master Key



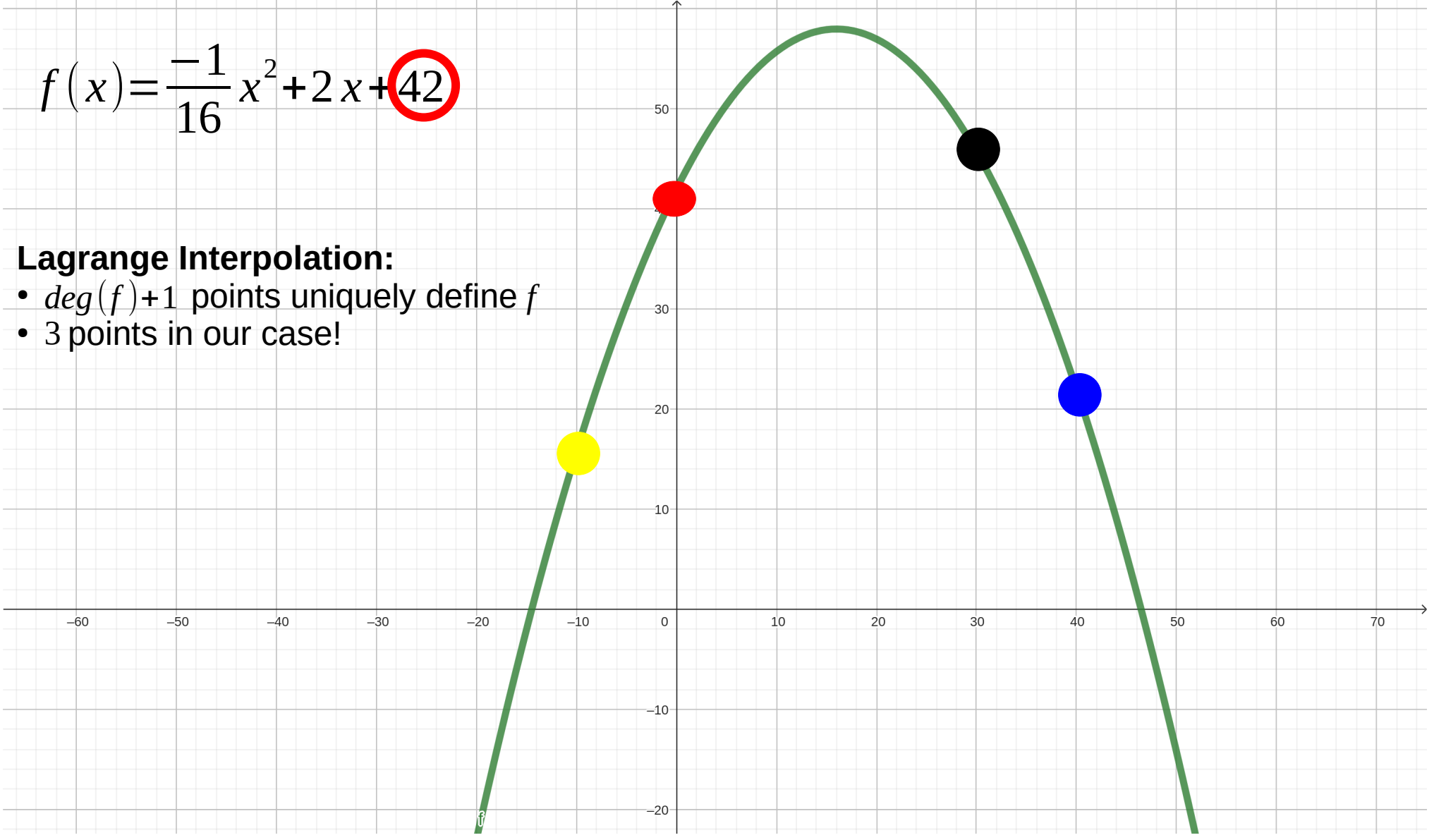
$$f(x)=\frac{-1}{16}x^2+2x+42$$



$$f(x)=\frac{-1}{16}x^2+2x+42$$

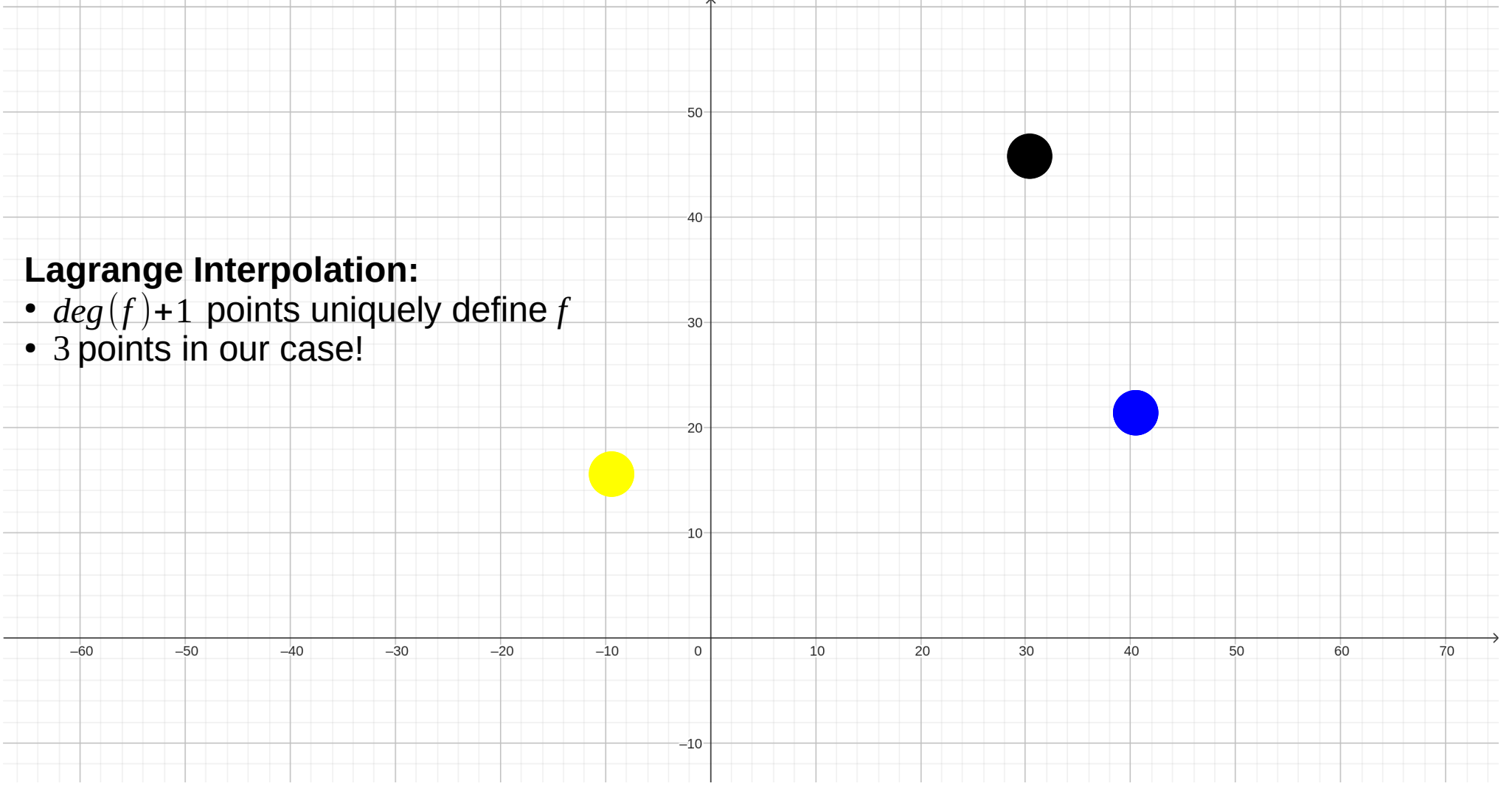
Lagrange Interpolation:

- $deg(f)+1$ points uniquely define f
- 3 points in our case!



Lagrange Interpolation:

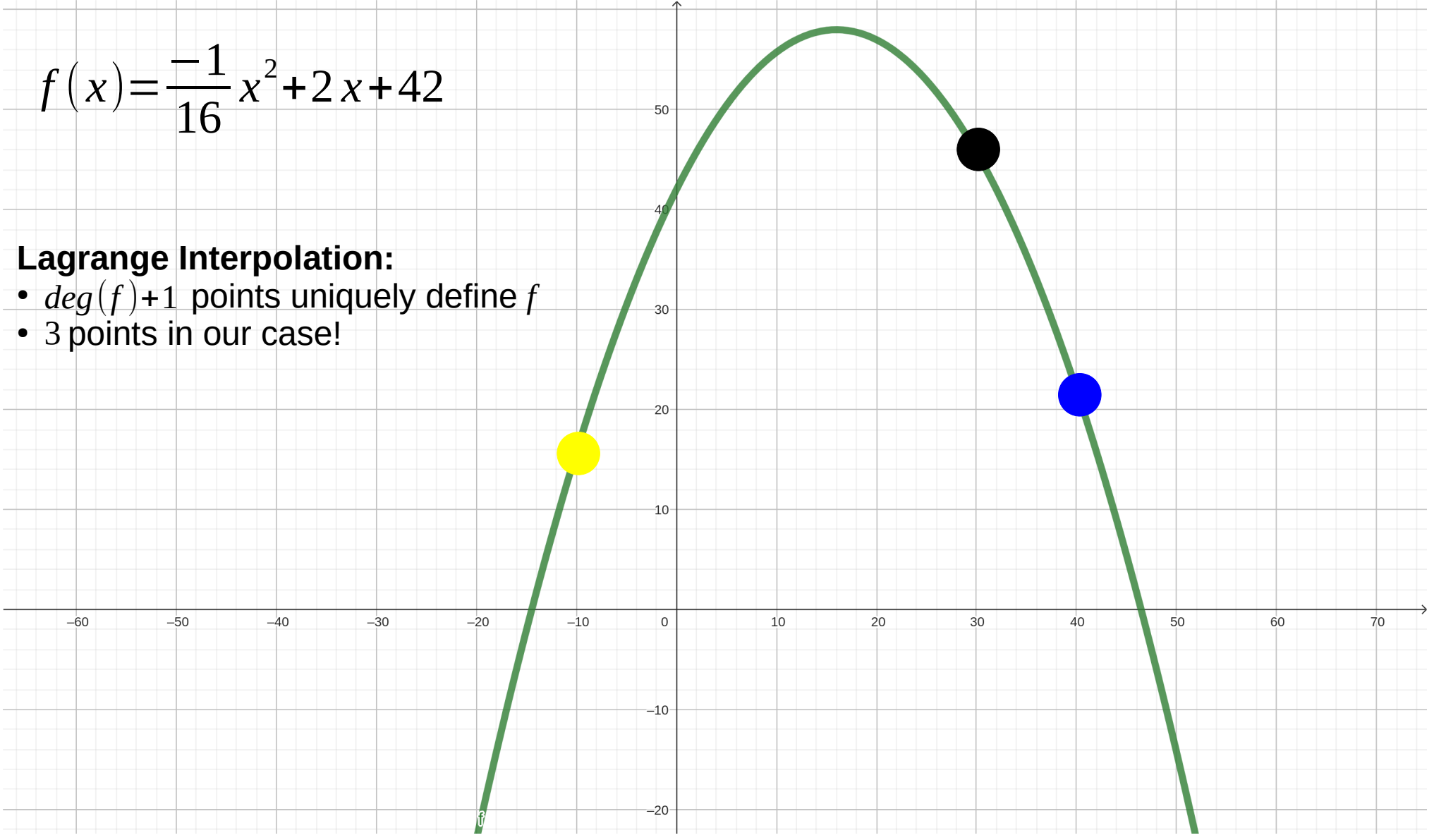
- $deg(f)+1$ points uniquely define f
- 3 points in our case!



$$f(x)=\frac{-1}{16}x^2+2x+42$$

Lagrange Interpolation:

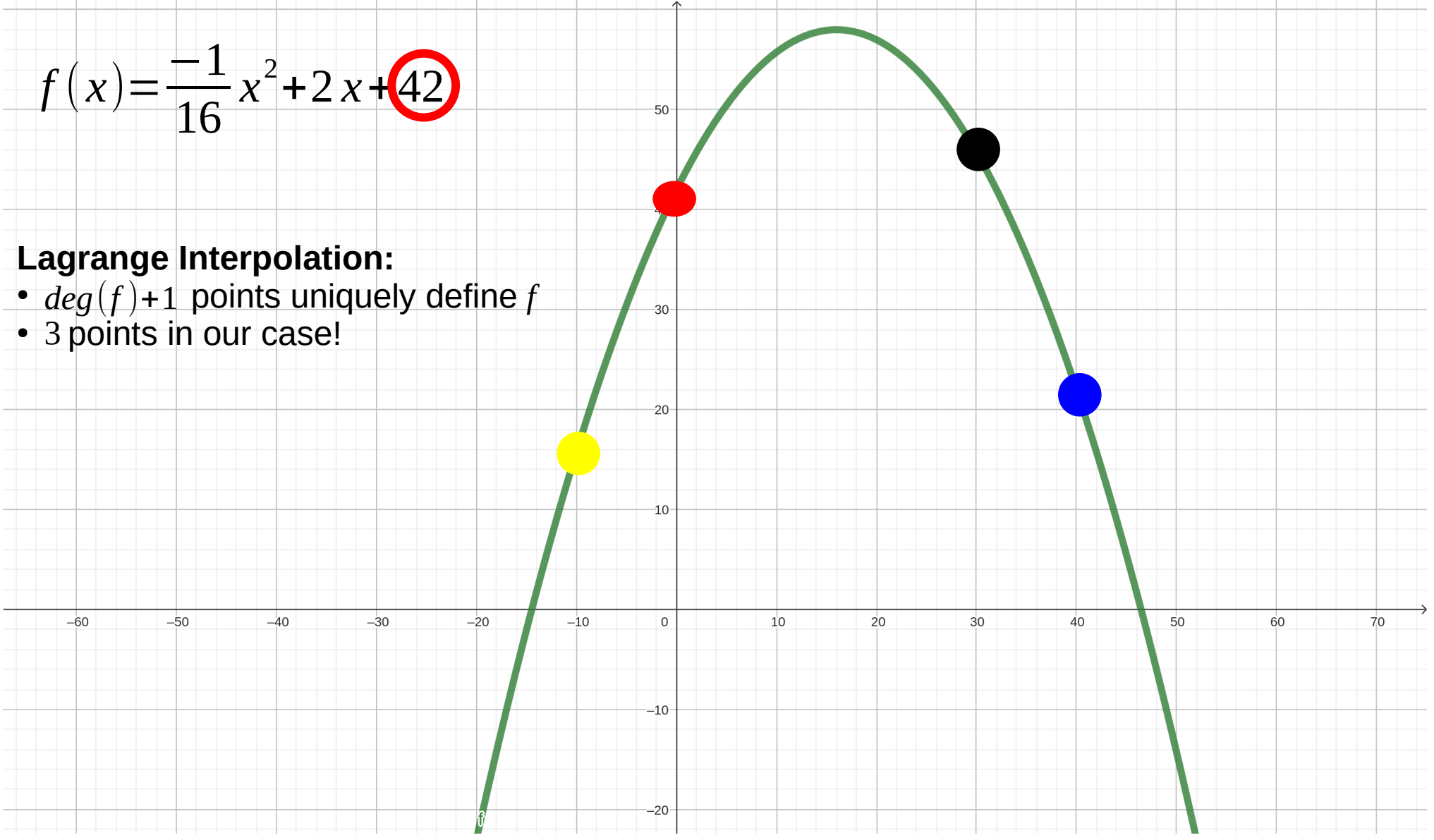
- $deg(f)+1$ points uniquely define f
- 3 points in our case!



$$f(x)=\frac{-1}{16}x^2+2x+42$$

Lagrange Interpolation:

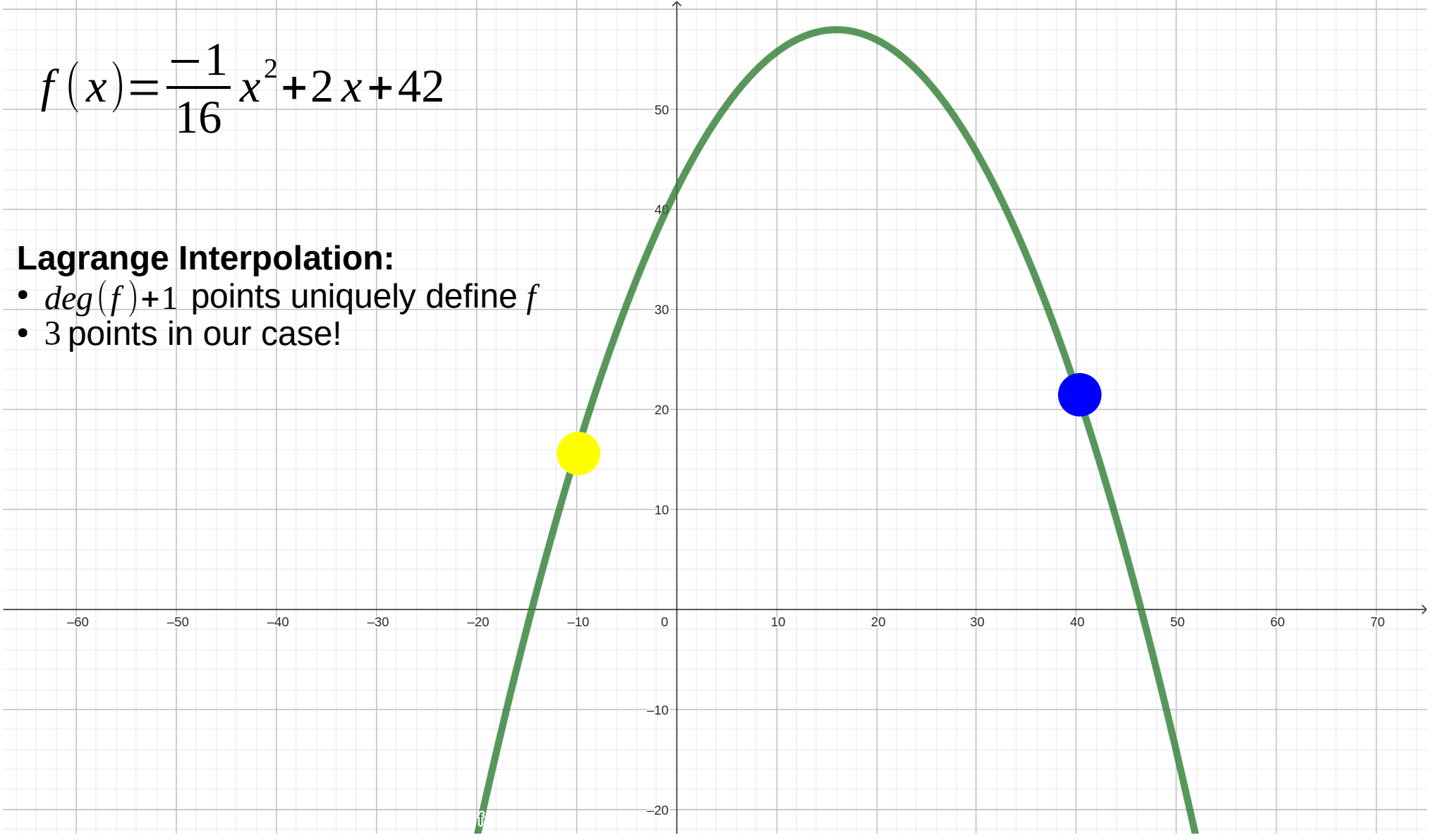
- $deg(f)+1$ points uniquely define f
- 3 points in our case!



$$f(x)=\frac{-1}{16}x^2+2x+42$$

Lagrange Interpolation:

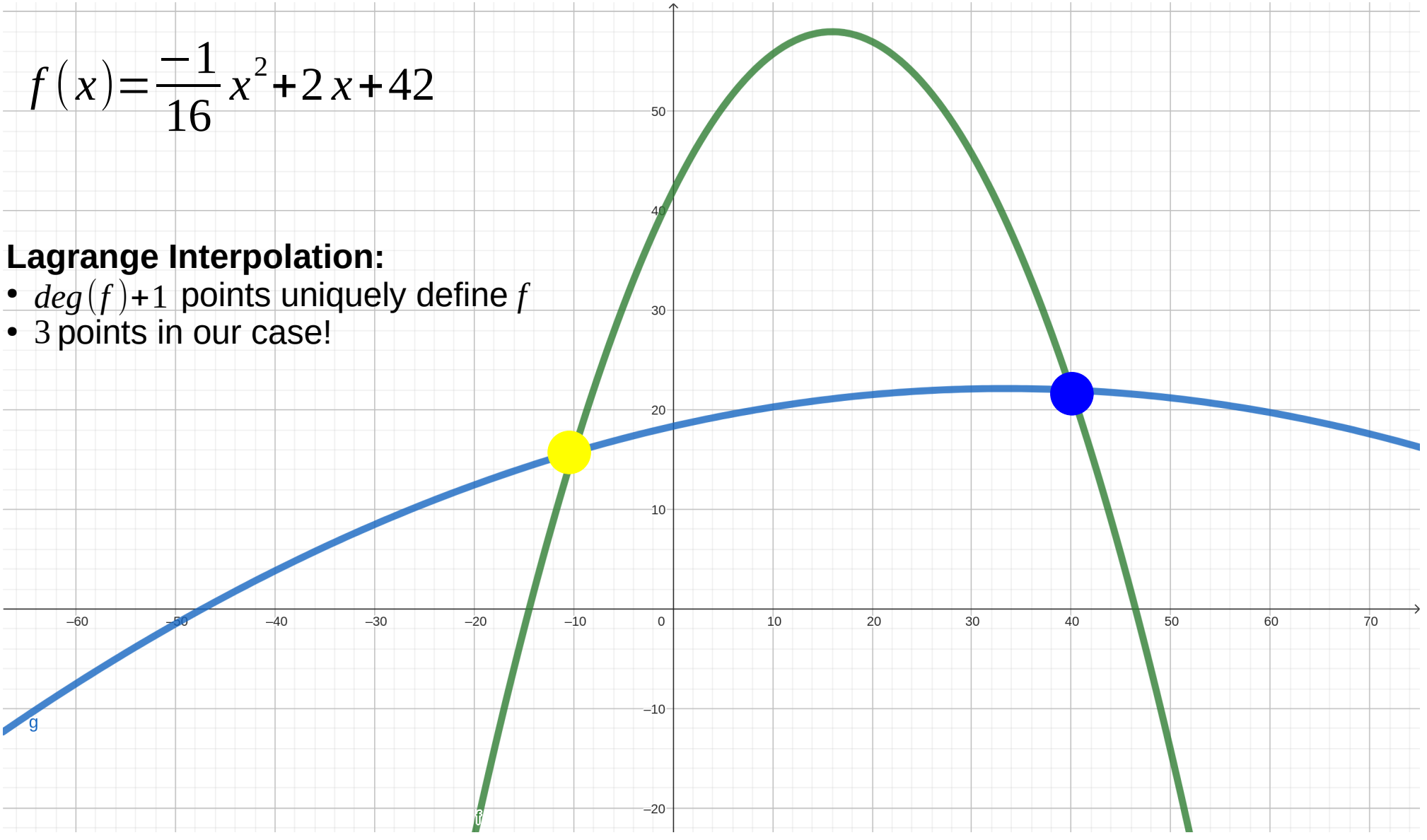
- $deg(f)+1$ points uniquely define f
- 3 points in our case!



$$f(x)=\frac{-1}{16}x^2+2x+42$$

Lagrange Interpolation:

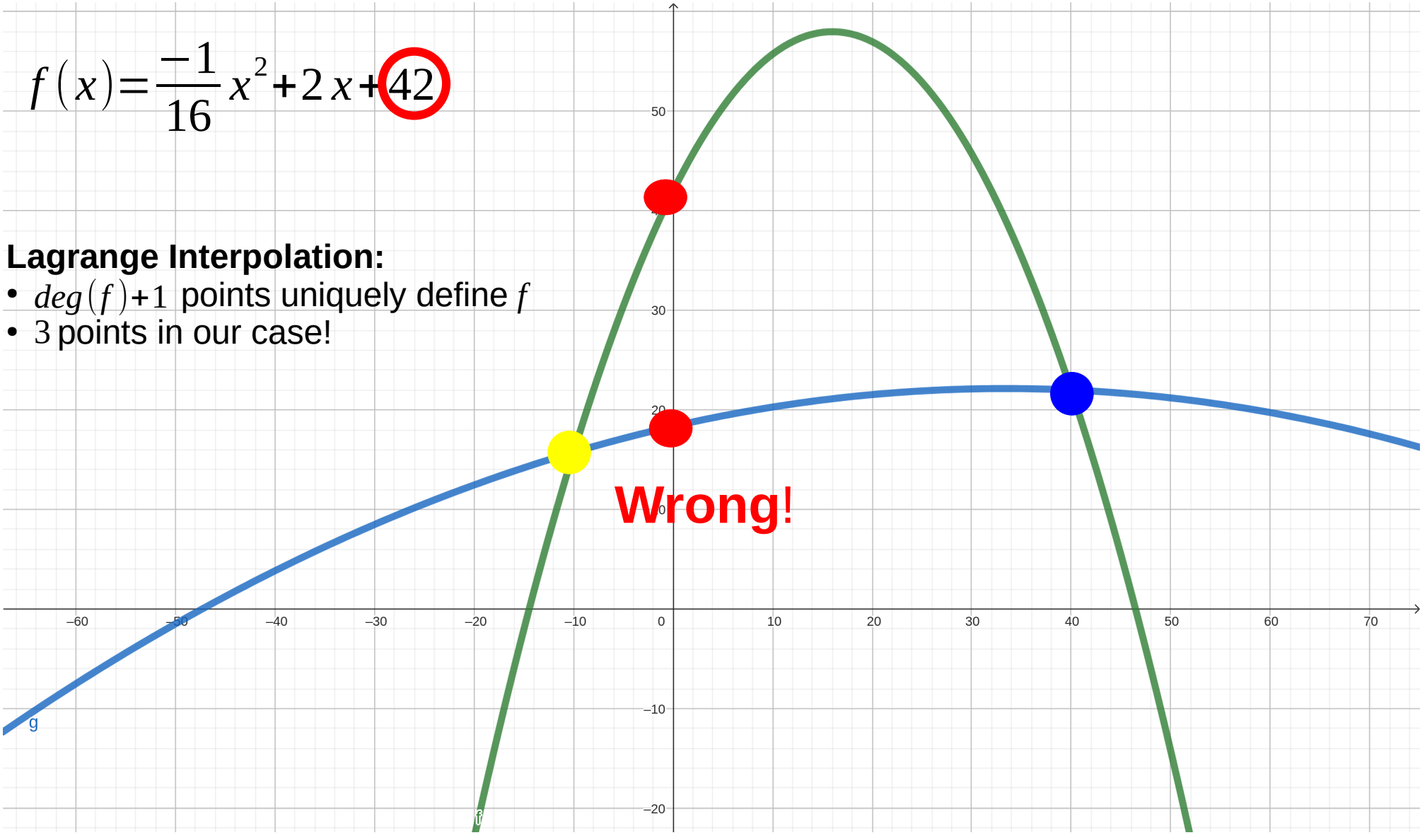
- $deg(f)+1$ points uniquely define f
- 3 points in our case!



$$f(x)=\frac{-1}{16}x^2+2x+42$$

Lagrange Interpolation:

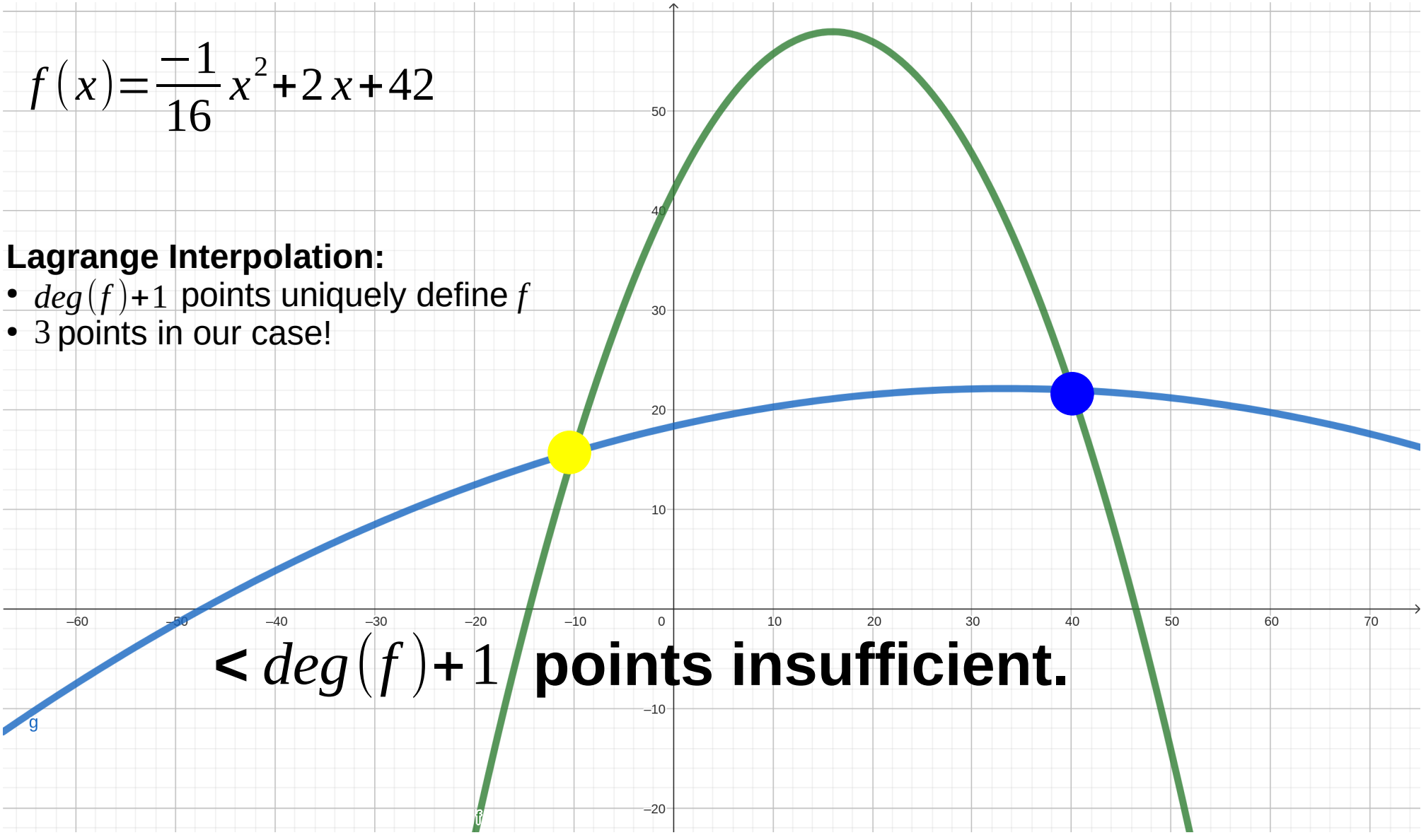
- $deg(f)+1$ points uniquely define f
- 3 points in our case!



$$f(x)=\frac{-1}{16}x^2+2x+42$$

Lagrange Interpolation:

- $deg(f)+1$ points uniquely define f
- 3 points in our case!

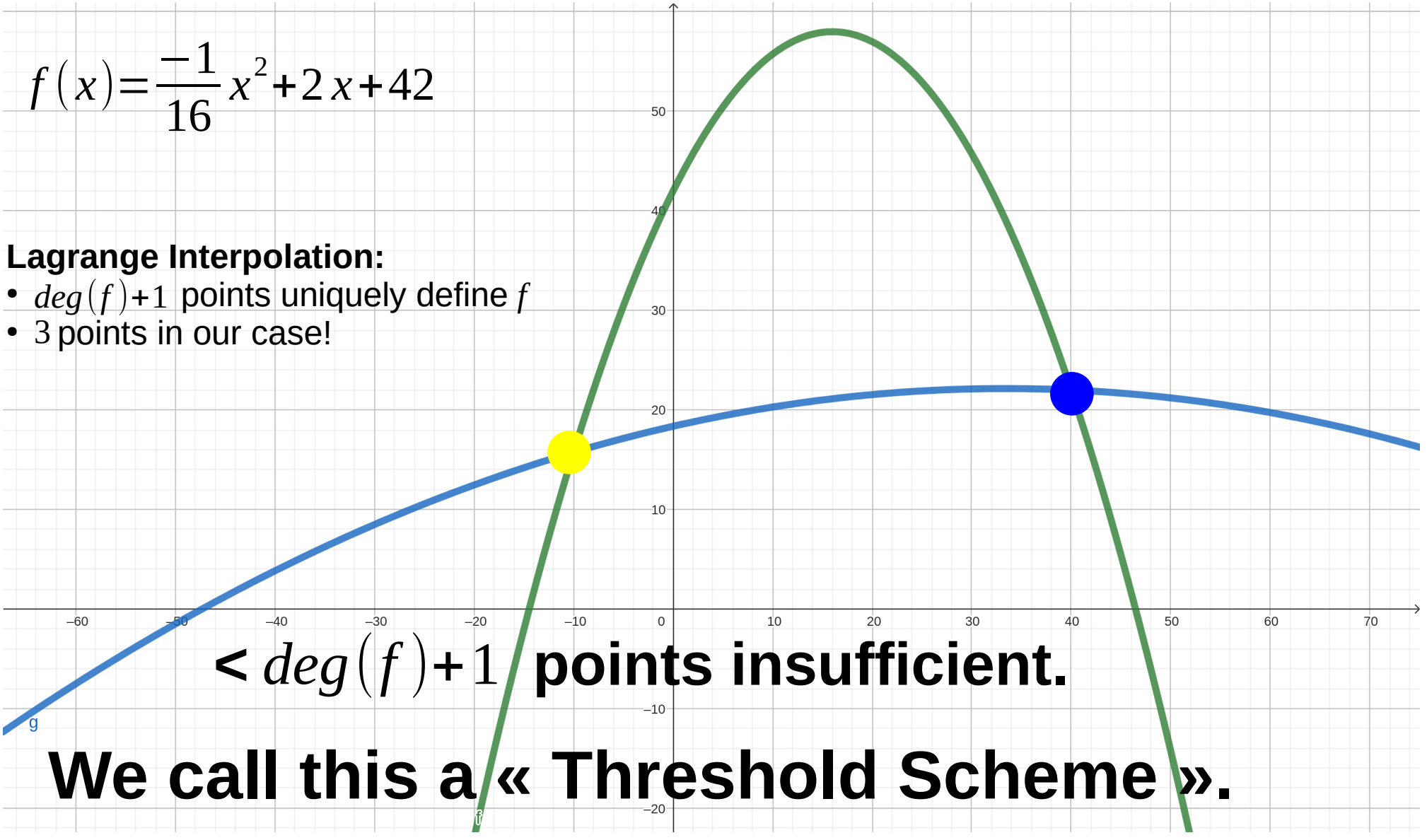


$< deg(f)+1$ points insufficient.

$$f(x)=\frac{-1}{16}x^2+2x+42$$

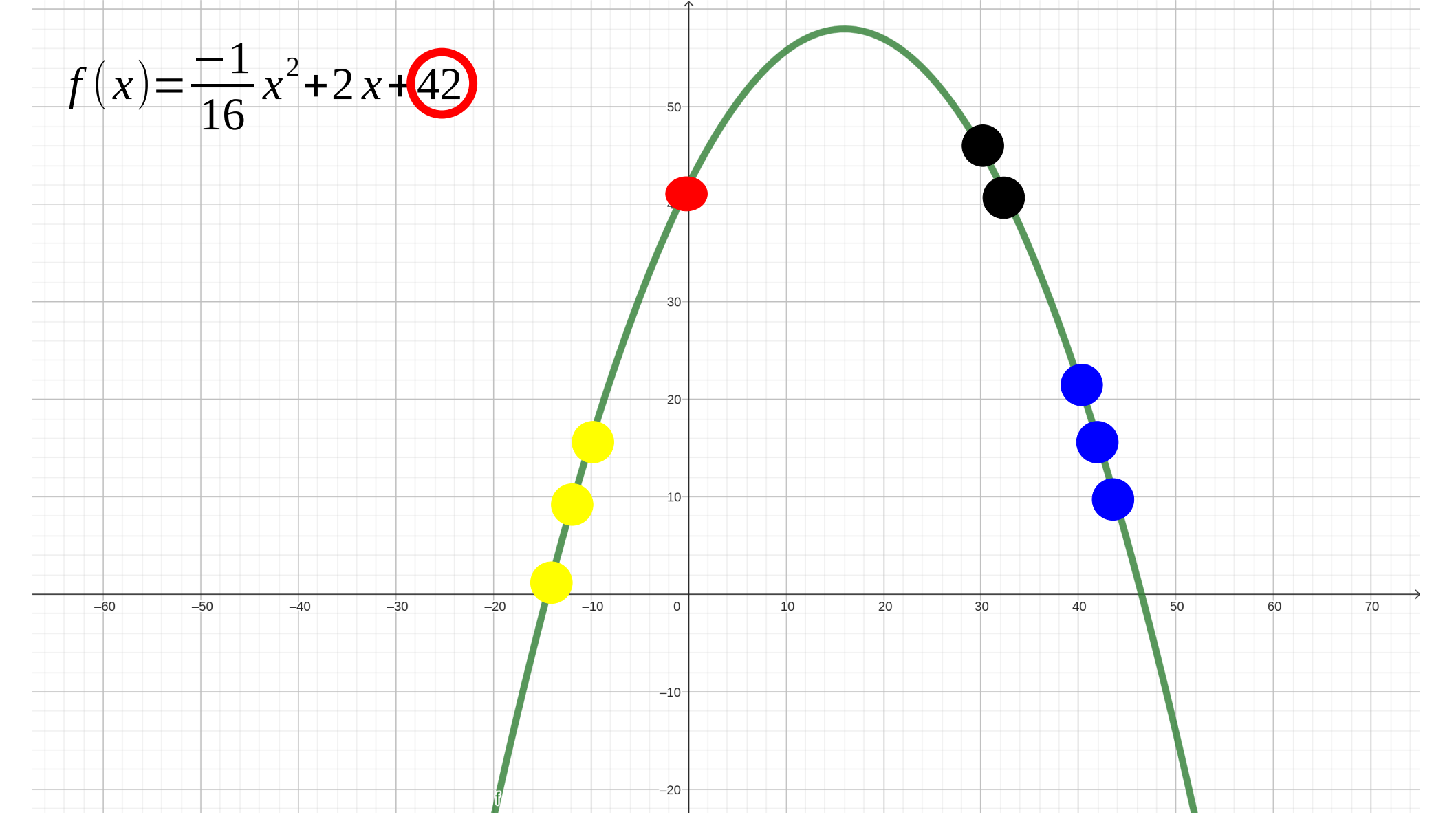
Lagrange Interpolation:

- $deg(f)+1$ points uniquely define f
- 3 points in our case!

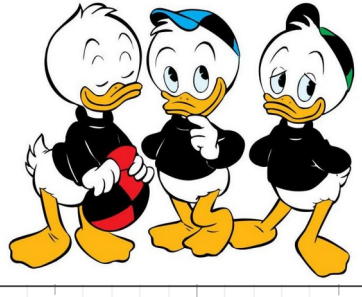


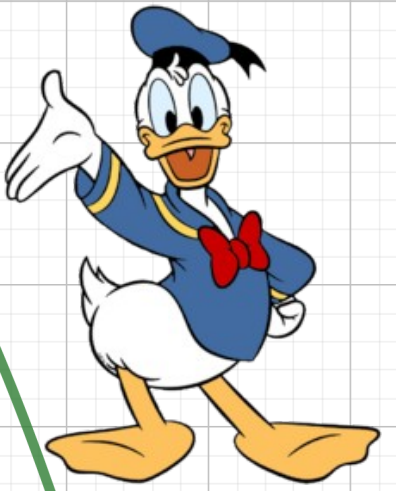
$< deg(f)+1$ points insufficient.

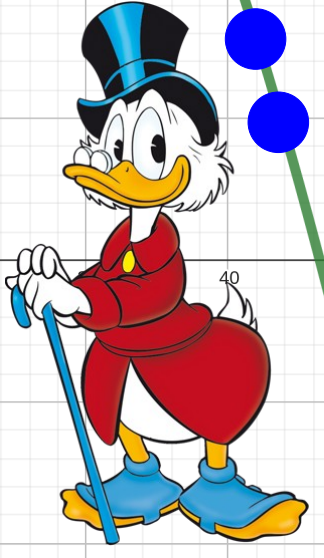
We call this a « Threshold Scheme ».


$f(x)=\frac{-1}{16}x^2+2x+42$
50
30
20
10
−10
−20
−60
−50
−40
−30
−20
−10
0
10
20
30
40
50
60
70

$$f(x)=\frac{-1}{16}x^2+2x+42$$

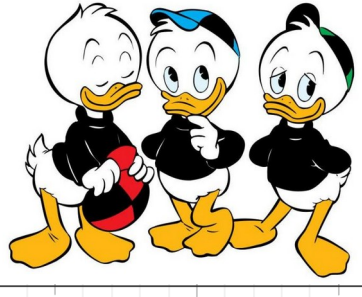


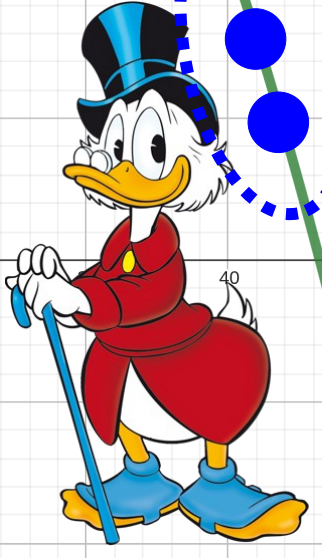




$$f(x)=\frac{-1}{16}x^2+2x+42$$

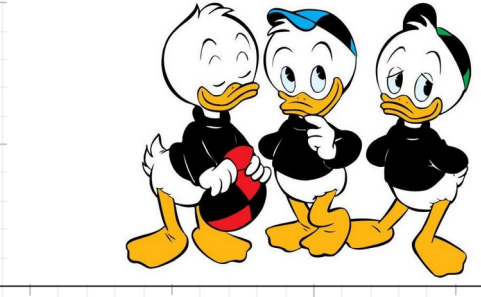
1. Hierarchical Access

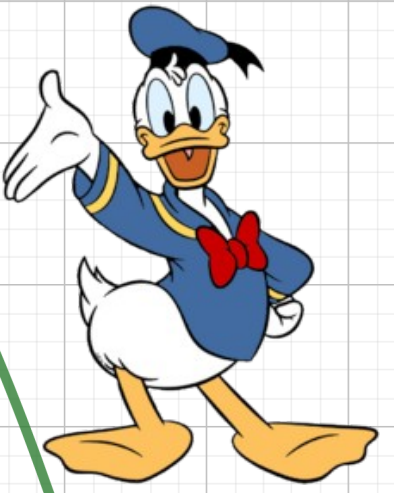


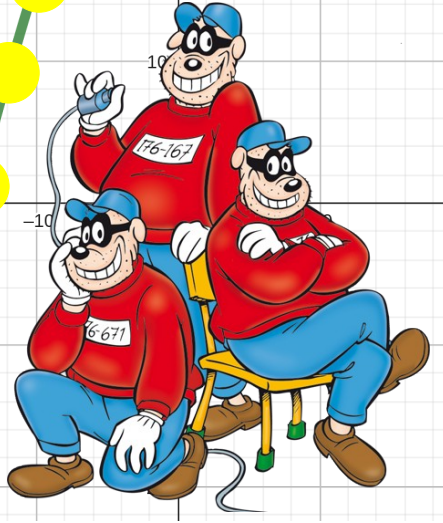


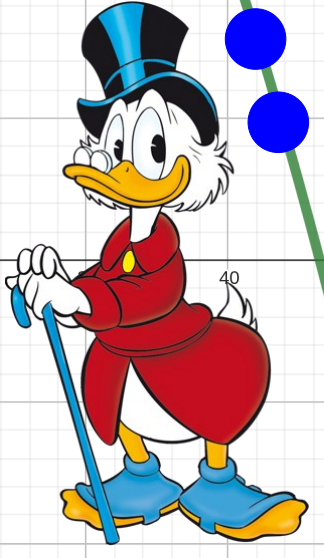
$$f(x)=\frac{-1}{16}x^2+2x+42$$

1. Hierarchical Access
2. Security Against Theft









How to Share a Secret:
Threshold Schemes!

How to Share a Secret:
Threshold Schemes!

Used in Secure Multi-Party Computation

Notable Use Case: Cryptocurrencies

Sources

https://www.dreamstime.com/cartoon-pile-gold-coins-pirate-gold-vector-illustration-pile-gold-coins-pirate-gold-vector-illustration-image169398347

https://www.freepik.com/free-photos-vectors/bank-flat

https://www.goldstories.com/de/glow/dagobert-duck

https://www.lustiges-taschenbuch.de/entenhausen/charaktere/die-ducks/dagobert-duck

https://toppng.com/pile-of-gold-coins-png-PNG-free-PNG-Images_115274

https://www.lustiges-taschenbuch.de/entenhausen/charaktere/die-ducks/dagobert-duck

https://www.welt.de/vermischtes/article169678495/Tick-Trick-und-Track-ihr-seid-nur-nervige-Streber.html

https://disney-junior-random-episodes.fandom.com/wiki/Donald_Duck

https://www.lustiges-taschenbuch.de/entenhausen/charaktere/die-ducks/die-panzerknacker

https://www.lustiges-taschenbuch.de/entenhausen/charaktere/die-ducks/daniel-duesentrieb

https://www.pinterest.fr/annwaa185/donald-duck-rocks/

https://www.lustiges-taschenbuch.de/entenhausen/charaktere/die-ducks/helferlein?character=1390&page=21

https://en.wikipedia.org/wiki/Zcash

https://disney.fandom.com/wiki/The_Money_Bin

https://uh.edu/facilities/news-and-events/stories-archive/2016/08/Extended%20Hours%20for%20Key%20Access%20Services.php

$$f(x)=\frac{-1}{16}x^2+2x+42$$